OFFICE OF SECRETARY OF STATE

DEPARTMENT OF HUMAN RESOURCES

ADMINISTRATIVE INVESTIGATION

FINDINGS PRESENTED
December 14, 2015

INVESTIGATION CONDUCTED BY
John Jurkiewicz
Director of Administration

David Dove
Assistant Deputy Secretary of State & Legal Counsel

INVESTIGATIVE MATTER
October 5-13, 2015, Voter Data Release

DIVISIONS
Information Technology Division
Elections Division

MATTER RECEIVED
November 13, 2015

TABLE OF CONTENTS

OVERVIEW

On November 13, 2015, at approximately 3:20 PM Secretary of State Brian Kemp was notified that voter registration data had been distributed containing personal identifying information of up to 6.1 million Georgia voters. Shortly thereafter, Secretary of State Brian Kemp ordered the Deputy Secretary of State, Tim Fleming to investigate and determine the facts leading to the data release.

An initial investigation determined that Gary Cooley, a systems programmer in the Secretary of State's IT Division, directed PCC Technology Group, the agency's elections software vendor, to add three additional fields -- the date of birth, social security number, and driver's license number -- to a download file containing voter registration information for each Georgia voter.

Although Mr. Cooley made the communications leading to the release of data, Secretary Kemp requested that the investigation look further to determine if any other employees violated agency policies and to present recommendations for changes moving forward.

SCOPE

This report addresses the policies and procedures as well as actions taken by employees of the Secretary of State's office and election vendors leading up to, during, and after the release of personal identifying information of Georgia's voters.

To gain an understanding of the events leading up to the release as well as why the release occurred, the investigation was authorized to research the personnel files and human resources records of employees. In addition, the investigation was authorized to research the contracts, agreements, and memoranda with vendors or contractors held by the Secretary of State's office.

The investigation was also authorized to research emails, correspondence, and other documents between employees in the agency as well as between employees and outside vendors or contractors. The investigation was also authorized to research all documents, notes, files, and other papers held by the agency related to events occurring between August 1, 2015 and November 13, 2015.

METHODOLOGY

This Investigation follows administrative review of the above-referenced matter. The investigative methodology used to review this matter regarding the October 5-13, 2015 IT/Elections Data Release was:

- Collect and examine Secretary of State (SOS) Policies specific to Release Management, Data Distribution, and staff confidentiality. **Exhibit C**
- Collect and examine Standard Operating Procedures related to Release Management and Data Distribution. **Exhibit C**
- Collect and examine job descriptions of those positions associated with data release and/or data distribution. **Exhibit B**
- Examine historical email records using "key word" search referenced in **Exhibits F & J**
- Develop relevant questions and conduct staff interviews pertaining to positions directly involved or associated with the October 5-13, 2015 IT/Elections data release. Additionally, request staff members provide a written summary of his/her interview to include relevant information.
- Contact vendor, ask associated questions relative to the data release, record responses and request a written statement summarizing the conversation. **Exhibits A & E**

Staff Interview Questions

1. **IT Division**
    a. How was this information disseminated to the IT staff?
    b. What documents or policy acknowledgements are on file for this?
    c. Based on the Data Distribution and Exchange Policy # SOS-ITP-36-3, what agreement or process mapping was provided to PCC?
    d. What document exists that maps process and approval for the Ongoing Exchange Agreement?
    e. How does the end user notify the third party that data is available?
    f. What is the notification process to the vendor when a file is ready for transfer?
    g. How is the Elections Division notified that the file is approved and ready to be loaded on a CD?
    h. Was PCC involved in the release management process of this project?
    i. What level of management or personnel was involved in this project?
    j. What level of management or personnel approved the transfer process?
    k. At the time of file transfer or after, did PCC contact SOS management or personnel regarding the content or question the request from Gary Cooley?
    l. Is there a document that outlines project deliverables and approval levels?
2. **Elections Division**
    a. What is the process for mailing or distributing electronic data via CD?
    b. Do you know how long this process has been in place?
    c. Who conducts this process?
    d. Before November 13, 2015, to your knowledge, was there a requirement to have the data reviewed for the inclusion of possible sensitive information?

e. To your knowledge, was the Elections Division notified that there would be a change to the statewide voter file download?

f. How is the Elections Division notified when the statewide voter file download is ready for use to be loaded on a CD?

g. What guidelines are in place for the Elections System Support Specialist to follow regarding transfer of elections data on a CD? Does this require manager approval?

h. Were you aware at the time before November 13, 2015 that the Georgia Department of Revenue requested a copy of the statewide voter file?

i. To your knowledge, was the Elections Division notified by IT or Legal of the Georgia Department of Revenue request?

j. Was the Elections Division involved in the Release Management process of the DOR project? If so, was the Elections Division notified that the file was approved and ready?

k. Did IT management and/or Gary Cooley mention the required/approved process regarding the new columns added to a file? If so, did Mr. Cooley or anyone in IT recommend any checks and balance due to the inclusion of confidential information?

STATEMENT OF FACTS

The following six sections of this report outline the facts uncovered by the internal investigation. These sections describe in detail the Statewide Download File, procedures for receiving the Statewide Download File, IT release management procedures and security protocols, the Secretary of State's office's data security training, Gary Cooley's employment record, and the timeline of events leading to the October 2015 data release.

Section 1: The Statewide Download File

The Statewide Download File (SDF), "statewide voter file," or the "daily file" as it is sometimes referred to, is the electronic voter roll for the state of Georgia. The SDF contains voter information that is a matter of public record such as a voter's name, voter registration number, and address.[1] The SDF contains both active and inactive electors' data. The SDF exists to provide voter information to the public, required pursuant to O.C.G.A. § 21-2-225. It does not contain Personal Identifying Information (PII) such as full dates of birth, social security numbers, or driver's license numbers.[2]

The SDF is stored on a secure file transfer protocol (SFTP) site.[3] Several folders exist on this SFTP site that serve as portals or interfaces where users can download voter information.[4] The information contained in each folder of this SFTP site varies depending on the user's needs and

[1] **Exhibit H**, Georgia Secretary of State's website, ORDER VOTER REGISTRATION LISTS AND FILES.
[2] *Id.*
[3] **Exhibit A**, Statements of Chris Harvey and Kevin Reaves.
[4] *See*, **Exhibit E**.

level of access.[5] The only folder on the SFTP site that is considered to contain the "Statewide Download File" is a folder entitled "statewide."[6]

The "statewide" folder was created by PCC Technology Group (PCC) to serve as a portal to share reports with the Secretary of State's IT Department, specifically, Gary Cooley.[7] PCC controls the number of users and grants log-in credentials.[8] The only user ever granted access to the "statewide" folder was Mr. Cooley.[9] Mr. Cooley was the only employee granted access to this file because of his singular and unique institutional knowledge of the mainframe system.[10] Because of his expertise, he had been identified on February 18, 2014 by the IT Division as the point of contact for PCC to work on migration projects.[11] PCC was unaware of any other users of this folder.[12]

Without PCC's knowledge, Mr. Cooley used his log-in credentials to give the Elections System Support Specialist in the Elections Division access to the SDF stored there.[13] The Elections System Support Specialist was unaware that Mr. Cooley had used his personal credentials in providing access.[14] Mr. Cooley did not create a separate folder for the Elections Division to access this file as was done for other entities that required information. This fact is very important to understanding the timeline in Section 6.

---

[5] *Id*.
[6] *Id*.
[7] **Exhibit A**, Statement of Keval Patel; *See*, **Exhibit E**.
[8] *Id*.
[9] *Id*.
[10] *See*, **Exhibit A**, Statements of Merritt Beaver and Erica Hamilton.
[11] **Exhibit E**.
[12] **Exhibit A**, Statement of Keval Patel; *See*, **Exhibit E**.
[13] *Id*.
[14] *See*, **Exhibit A**, Statement of Kevin Reaves.

The Elections Division uses the SDF to produce voter lists to send to parties that request it.[15] Once successfully connected with the secure SFTP site, the Elections System Support Specialist may then copy the file for distribution.[16] The file is distributed on a non-encrypted CD-ROM. The disc is not encrypted because the information contained on the file, in the normal course, is public and does not contain PII. These discs are mailed from the Secretary of State's mailroom in sealed cardboard disc covers, placed in a sealed bubble-wrap mailer.[17]

Within the first two weeks of every month, this file is distributed to political parties and news organizations that have registered with the Secretary of State's Elections Division (please see section 2 for details on these parties and how they register.).[18] Files are also sent to parties that purchase the list of statewide electors, although these purchases do not tend to occur on a regular basis (please see section 2 for additional details on these purchases.).[19]

Section 2: Receiving the Statewide Download File

In accordance with O.C.G.A. § 21-2-225, the SDF is available to the public.[20] The file is available for purchase by any member of the public via order form on the Georgia Secretary of State's website: http://sos.ga.gov/index.php/elections/order_voter_registration_lists_and_files.[21]

In addition, political parties or news organizations could register with the Georgia Secretary of State's Elections Division to receive a free copy of the SDF.[22] Until November 16, 2015, a disc containing the SDF was sent within the first two weeks of each month to registered

[15] **Exhibit A**, Statement of Chris Harvey.
[16] **Exhibit A**, Statements of Kevin Reaves and Mike Myers.
[17] *See*, **Exhibit A,** Statement of Mike Myers; *See***, Exhibit H**.
[18] **Exhibit A**, Statements of Chris Harvey and Jessica Simmons.
[19] **Exhibit H**, Records of Voter List Transactions.
[20] *Id*, Georgia Secretary of State's website, ORDER VOTER REGISTRATION LISTS AND FILES.
[21] *Id*, for a copy of the voter list order form, *see* **Exhibit H.**
[22] *See*, **Exhibit A**, Statements of Chris Harvey, Jessica Simmons, Kevin Reaves, and Mike Myers.

recipients.[23] At the time of the data release, twelve entities were registered to receive a free copy of the SDF.[24] The entities are: the Georgia Democratic Party, the Georgia Republican Party, the Georgia Libertarian Party, the Independence Party of Georgia, the Southern Party of Georgia, the Atlanta Journal-Constitution, the Macon Telegraph, the Savannah Morning News, Georgia GunOwner Magazine, Georgia Pundit, News Publishing Co., and Peach Pundit.[25]

Pursuant to the order of Secretary of State Brian Kemp, the list of registered entities receiving a copy of the SDF has been reset.[26] At the time of this report, no entity has yet reapplied to receive a copy of the SDF.

Section 3: IT Release Management Procedures and Security Protocols

The Information Technology Division for the Georgia Secretary of State's office has procedures in place to direct the activities of employees both with securing sensitive data as well as through release management. These policies have developed at the direction of Secretary of State Brian Kemp. Prior to his taking office, IT governance policies did not exist. The introduction of these policies helped bring the Secretary of State's IT Division into alignment with industry standards. All IT policies and procedures are included in **Exhibit C**.

Section 4: Data Security Training

In the first half of 2015, the Georgia Secretary of State's office underwent agency-wide mandatory data security training.[27] The office contracted with SANS, a national leader in data

[23] *Id.*
[24] *See*, **Exhibit H**.
[25] *Id.*
[26] *See*, **Exhibit K.**
[27] *See*, **Exhibit A**, Statement of James Oliver; **Exhibit D**, SANS Report.

security management to provide training courses as well as training documents.[28] From the SANS website, www.sans.org, the company describes itself as follows:

> *The SANS Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. A range of individuals from auditors and network administrators, to chief information security officers are sharing the lessons they learn and are jointly finding solutions to the challenges they face. At the heart of SANS are the many security practitioners in varied global organizations from corporations to universities working together to help the entire information security community.*
>
> *SANS is the most trusted and by far the largest source for information security training and security certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - the Internet Storm Center.*[29]

The SANS course consisted of thirteen modules. However, employees were only required to complete modules selected for their division.[30] IT Division employees were required to complete "Introduction," "You Are the Target," "Passwords," "Data Security," "Working Remotely," "IT Staff," "End," and for those to whom it applied, "Help Desk."[31] A completion log was tracked by SANS during the course.[32] Each time an employee completed a module of the

[28] **Exhibit D**, SANS Report.
[29] ABOUT SANS, https://www.sans.org/about/ (Last Accessed Dec. 11, 2015, 4:33 PM).
[30] **Exhibit D**, SANS Report.
[31] *Id*.
[32] *Id*.

course, the file was date stamped.[33] Gary Cooley completed all of his required modules on March 17, 2015.[34]

Training materials from SANS were not available at the time of this report because they must be licensed for use.[35] However, all relevant documents related to the SANS training course are included at the end of this report in Appendix D. The company also has some materials available on its website, www.sans.org.

Section 5: Gary Cooley's Employment Record

Gary Cooley was hired by the Secretary of State's office on December 16, 2008.[36] Prior to that time, Mr. Cooley was a senior programmer/analyst with Comprehensive Computer Consultants, a contractor with the Secretary of State's office.[37] Mr. Cooley had worked in that capacity with the Secretary of State's office since 1995.[38]

Mr. Cooley's job description, last updated September 4, 2013, outlined his responsibilities, notably including: "Prepares detailed workflow charts and diagrams that describe input, output, and logical operations … Compiles and writes documentation of program development … Consults with others to clarify program intent, identify problems, and suggest changes."[39] In addition, the required knowledge, skills, and abilities description includes "Knowledge of change management process of the agency."[40]

[33] *Id.*
[34] *Id.*
[35] ABOUT SIC – SANS INNOVATION CENTER, https://sic.sans.org/about (Last Accessed Dec. 11, 2015, 4:36 PM).
[36] **Exhibit I**, Gary Cooley's Personnel File.
[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] *Id.*

On August 10, 2009, only eight months after being hired, Mr. Cooley was suspended without pay by his supervisor for failure to achieve accuracy in his work, failing to document audit processes, and failing to accurately and timely communicate his work flow to his supervisor.[41] In all, Mr. Cooley's supervisor developed an 8-point plan that Mr. Cooley was required to follow to ensure his work met the expectations of the office.[42]

The eight points included in Mr. Cooley's performance plan contained information relevant to this investigation. Mr. Cooley was instructed in the following: "From now forward, any external release of numbers must have the highest standard of review and accuracy." The personnel file reflects that Mr. Cooley had procedural issues with the process of release management and publishing accurate data.[43] He was instructed that the level of scrutiny required by his position for his work was very high.[44] Much depended on Mr. Cooley's accurate reporting of data as is now seen by this most recent incident in October 2015.[45]

Moreover, Mr. Cooley was required to create and maintain mandatory development procedures.[46] This process required Mr. Cooley to document his actions on all reports, to meet with his supervisor and explain his actions, and to circulate emails explaining his actions.[47] These requirements were intended to prevent Mr. Cooley from coding something incorrectly or providing inaccurate or incorrect data.[48] These actions were not followed in this instance.

[41] *Id.*
[42] *Id.*
[43] *Id.*
[44] *Id.*
[45] *Id.*
[46] *Id.*
[47] *Id.*
[48] *Id.*

This tendency to act independently continued to persist in Mr. Cooley. The Chief Information Officer and the Deputy Chief Information Officer, Mr. Cooley's direct supervisor, both acknowledged that Mr. Cooley was independently minded in his work processes.[49] Procedures required by the IT Division for release management and governance were not readily accepted by Mr. Cooley.[50] Although no formal disciplinary action was taken, Mr. Cooley regularly had meetings with his superiors where he was instructed to follow agency and division policies in his work.

Section 6: Timeline of Events

Fall 2014 – Summer 2015

On August 1, 2014, the Secretary of State's office received a request from the Georgia Department of Revenue for a new interface with the Statewide Download File held by the Georgia Secretary of State's office.[51] The Department of Revenue has for years received a voter file with voter information for match purposes with its database.[52] While the Secretary of State's office was on a mainframe data system, this report was generated manually each January by Gary Cooley.[53]

The Secretary of State's IT Division had since early 2014 been involved with migrating data processes from the older mainframe system to a server-based system.[54] This report for the Department of Revenue was one of the last projects to be migrated over from the mainframe

[49] **Exhibit A**, Statement of Merritt Beaver.
[50] *Id.*
[51] **Exhibit G**, JIRA Ticket ELCT-442.
[52] *See*, **Exhibit F**.
[53] **Exhibit I***; See*, **Exhibit A**, Statements of Merritt Beaver, Erica Hamilton, and Mike Myers.
[54] **Exhibit A**, Statements of Merritt Beaver.

system. Because of this request by the Department of Revenue in August 2014, this migration gained a priority status.[55]

The Department's request was entered into JIRA, the Secretary of State's office's project management ticketing system, and given the name ELCT-442.[56] Several initial steps were taken by IT employees, but no substantial work was completed on the project.[57] Another JIRA ticket subsequently was created for the project, AR-102.[58] After additional communications with the Department of Revenue, both tickets were closed on November 6 and November 10, 2014, respectively.[59]

August 6, 2015

On August 6, 2015, an IT employee from the Georgia Department of Revenue contacted Gary Cooley and renewed the Department's request for a copy of the SDF that included PII for all Georgia voters.[60] The specific information the Department requested was full date of birth, driver's license numbers, and full nine-digit social security numbers.[61]

On August 6, Gary Cooley emailed Farah Allen, the Project Manager for the Department of Revenue's JIRA ticket.[62] Ms. Allen recommended that they contact the agency's legal division to inquire as to the legality of sharing the information in the request before moving forward.[63] Ms. Allen contacted Candice Broce, staff attorney for the Elections Division that afternoon.[64]

---

[55] **Exhibit G**, JIRA Ticket ELCT-442.
[56] *Id.*
[57] *Id.*
[58] **Exhibit G**, JIRA Ticket AR-102.
[59] **Exhibit G**, JIRA Ticket ELCT-442; JIRA Ticket AR-102.
[60] *See*, **Exhibits F & J**.
[61] *Id.*
[62] *Id.*
[63] *See*, **Exhibit F.**
[64] *Id.*

August 10-12, 2015

At some point in early August between August 6 and August 10, James Oliver, the Security Manager for the Secretary of State's IT Division, was informed of the project. On August 10, he emailed PCC, the system vendor for the Georgia Voter Registration System, to begin discussions about the security infrastructure needed to accommodate the Department of Revenue's request.[65] In his email, he noted that the normal process for conveying this information to counties is through a secure file transfer protocol (SFTP).[66] Keval Patel with PCC acknowledged that this is the system used for file transfers with counties and that PCC could build an SFTP file for use by the Department of Revenue.[67]

Also on August 10, JIRA ticket ELCT-442 was reopened by Gary Cooley.[68]

After the email thread of the August 10, 2015, Mr. Oliver called Mr. Patel on the 11th to discuss in greater detail the SFTP transfer.[69] The two also discussed the process by which the Georgia Elections Division receives the SDF, noting that it was not encrypted as it does not contain personal data.[70] After the call Mr. Oliver emailed Merritt Beaver, the Chief Information Officer for the Georgia Secretary of State's office, to describe his conversation. A relevant portion of the email is as follows:

> *Based on my conversation with Gray Cooley* [sic] *the information provided in this file (Department of Revenue File) is different from the data release to the general public. This data contains the complete DOB, Names, and Addresses which by definition make the data*

[65] *Id.*
[66] *Id.*
[67] *Id.*
[68] **Exhibit G**, JIRA Ticket ELCT-442.
[69] *See*, **Exhibit F.**
[70] *Id.*

PII. PII data is required to be protected (encrypted) in transit and at rest if stored in the open (DMZ), which the general public can access. The DOR will contain lots more sensitive items in the data, but we did not discuss this because Keval stated PCC has not received any requirements on that task yet. The two key points to take away are below:

1. If the complete DOB is needed/required the data should be protected both in storage and transit.

2. Some form of authentication should be in place to validate who received said data.

3. The owner of the data is responsible for the data (Secretary of State Office).[71]

It should be noted that in this email, Mr. Oliver references the release management process that requires formal requirements to be sent to the vendor before any work begins on the project. For more information on IT policies and release management, please see **Exhibit C**.

On August 11, 2015, Ms. Allen was informed that the Department's request included adding social security numbers to the data fields provided in the report. [72] Ms. Allen again contacted Ms. Broce.

Later, Rick Gardner, Deputy General Counsel for the Georgia Department of Revenue, contacted Ms. Broce by email introducing himself and inquiring whether a memorandum of understanding may be required to proceed with the request.[73] Ms. Broce replied to Mr. Gardner, copying Ryan Germany, the Secretary of State's office's General Counsel, to work with Mr. Gardner on the creation of an MOU.[74]

[71] **Exhibit F.**
[72] *Id.*
[73] *Id.*
[74] *Id.*

On August 12, through a discussion via email, it was determined by Mr. Gardner and Mr. Germany that in accordance with O.C.G.A. §§ 21-2-225 and 50-18-70 *et seq.*, an MOU was not required to proceed with sharing personal data between the government agencies.[75]

Later on August 12, Abraham Abutair, an IT Developer at the Georgia Department of Revenue, emailed Gary Cooley directly, noting that the Department must have all nine digits of the social security number for voters, otherwise the Department's matching process would not be successful.[76]

August 12 – October 1, 2015

On August 26, 2015, Mr. Abutair emailed Mr. Cooley asking to be kept apprised of the progress on the report of voters.[77] Also, during the intervening time, the Department of Revenue request was added to the list of projects for the IT Division.[78] Although the project maintained a priority status, progress was slow.[79]

It is important to note that through September 2015, all actions by all employees related to the Department of Revenue file request were in accordance with the IT Division's governance and release management procedures. All required authorizations and steps were being taken to ensure that when the data was provided to the Department of Revenue, it would be secured and delivered directly to the Department via a SFTP site.

October 1, 2015

[75] *Id.*
[76] **Exhibits F & J.**
[77] *Id.*
[78] *See*, **Exhibit G**.
[79] **Exhibit G**; *See*, **Exhibit J**.

On October 1, 2015, Mr. Cooley received a phone call from Charlette Uqdah, an IT Manager at the Georgia Department of Revenue.[80] The nature of their phone call was to follow up on the progress of the file being made available to the Department.[81] At that time, an SFTP site had been created to serve the needs of the Department; however, no file had yet been made available for download.[82]

October 3, 2015

On October 3, 2015, Mr. Cooley called Keval Patel at PCC.[83] Mr. Cooley instructed Mr. Patel that that the Department of Revenue needed its file sooner than it could be produced going through the normal channels of project release management.[84] Of note, if completed as initiated and intended the project would have resulted in a file with the requirements given by the Department being placed into a special SFTP site where only the Department would have had access to the information.

To accommodate the needs of the Department, Mr. Cooley asked Mr. Patel to produce a one-time report.[85] This report was intended to be a file with all the information needed by the Department for their purposes.[86] Mr. Patel instructed Mr. Cooley that in order to produce this type of report, he would need to send an email that copied Mr. Beaver, the CIO, and Ms. Allen, the project manager.[87]

October 5, 2015

---

[80] **Exhibits F & J.**
[81] *Id.*
[82] *Id.*
[83] *Id.*
[84] *Id.*
[85] *Id.*
[86] *Id.*
[87] **Exhibit A**, Statement of Keval Patel.

On October 5, 2015, Mr. Cooley emailed Mr. Patel regarding the report for the Department.[88] The full text of the email is listed below.

> *Keval, as we discuss* [sic] *can you add the 3 fields(full dob, ssn, and dl number) to the statewide down file layout to accommodate the DOR request. We would like this file to be create* [sic] *right as soon as possible. We can discuss the full automation from the application later. Thank you.*[89]

On the same day, Mr. Patel updated the SDF with the data requested by Mr. Cooley.[90] As a point of background, the SDF exists in a folder titled "statewide."[91] PCC understood at the time that only Mr. Cooley had the credentials to access this folder.[92] This is the folder Mr. Cooley gave the Elections Division access to for the production of SDF discs to be sent to the public.[93] However, PCC was not aware that Mr. Cooley had shared his user ID with another employee in the Secretary of State's office.[94]

Per a meeting on February 18, 2014, the "statewide" folder had been created for Mr. Cooley to receive reports from PCC.[95] PCC created and managed user IDs for access to the secure SFTP site. Rather than obtaining credentials for the Elections Division user, Mr. Cooley had merely signed the Elections Division user into the SFTP site using Mr. Cooley's credentials. The Elections Division employee was not aware that Mr. Cooley had used his own personal credentials to provide

[88] **Exhibits F & J.**
[89] *Id.*
[90] *Id.*
[91] See Section 1 above.
[92] **Exhibit A**, Statement of Keval Patel.
[93] *See*, **Exhibit A**, Statements of Mike Myers and Kevin Reaves.
[94] **Exhibit A**, Statement of Keval Patel.
[95] **Exhibit E**, PCC Reports.

access.[96] Both employees had received SANS training on passwords.[97] Mr. Cooley completed his training on March 17, 2015, and the Elections Systems Support Specialist completed training on June 15, 2015.[98] For more information on the SFTP file transfer process, please see Section 1 above.

Mr. Patel at PCC understood Mr. Cooley's October 5, 2015 e-mail instruction as a request to update the file contained in Mr. Cooley's "statewide" shared reports folder. PCC fulfilled this action, yet Mr. Cooley did not check the file to find the update. It appears that Mr. Cooley did not check the SDF because he expected PCC to create a new file with the requested information on it.

October 13, 2015

On the morning of October 13, Mr. Cooley contacted Mr. Patel to inquire when the request from October 5 would be processed.[99] His email at 9:30 AM read, "Keval, did you forget about me. We need this DOR interface file which includes the statewide file with the dob, ssn, and dl number added to the end of each record."[100] Mr. Patel replied at 9:40 AM, "It is done on the same day."[101]

After this email exchange, Mr. Cooley contacted Mr. Patel to ask that he immediately return the SDF to its original format.[102] However, prior to PCC removing the additional information from the SDF, the Elections Division had downloaded the SDF to burn copies of the file for the twelve parties that received a monthly copy of the SDF.

[96] *See*, **Exhibit A**, Statement of Kevin Reaves.
[97] **Exhibit D**, SANS Training Completion Certification Report.
[98] *Id.*
[99] **Exhibits F & J.**
[100] *Id*.
[101] *Id*.
[102] **Exhibit A**, Statement of Keval Patel.

Mr. Cooley did not notify anyone that the SDF had contained personal identifying information for the period from October 5 to October 13, 2105. Mr. Cooley claims that he checked to see if the file had been exported by another user. However, his check proved incomplete. In fact, Mr. Cooley gave the following statements to the media:

> *I thought the data may have ended up on the discs. I wish I would have said something. But when I checked, it looked like the problem had been resolved. I honestly didn't think there was a problem.*[103]

> *I admit I'm kicking myself for not walking over. That's the thing I regret.*[104]

If Mr. Cooley had chosen to mention the data issue to his supervisor, project manager, security manager, the elections director, the elections systems manager, or any employee involved with the project, the discs likely could have been recovered before they were even mailed. Instead, Mr. Cooley chose to cover up his mistake and remain quiet.

November 13, 2015

On November 13, 2015, at approximately 3:20 PM, Secretary of State Brian Kemp received a phone call from Todd Rehm at GA Pundit.[105] On that call, Mr. Rehm alerted Secretary Kemp that a disc he had received from the Elections Division included the date of birth, driver's license number and social security number for Georgia voters.[106]

---

[103] Shirek, Jon. GA SEC. OF STATE OFFERS FREE CREDIT MONITORING FOLLOWING DATA BREACH; FIRED WORKER SAYS HE'S A SCAPEGOAT, http://www.11alive.com/story/news/politics/elections/2015/12/03/sec-state-offer-free-credit-monitoring-following-data-breach/76745754/ (Dec. 3, 2015).
[104] *The Atlanta Journal-Constitution*, FIRED KEMP WORKER SAYS HE'S A SCAPEGOAT IN DATA BREACH, http://www.myajc.com/news/news/state-regional-govt-politics/exclusive-fired-kemp-worker-says-hes-a-scapegoat-i/npbCz/ (Dec. 2, 2015).
[105] **Exhibit A**, Statement of Brian Kemp.
[106] *Id*.

Immediately after being alerted of the issue, Secretary Kemp called David Dove, Assistant Deputy Secretary of State, to alert him of the inclusion of data on at least one statewide file.[107] Mr. Dove then informed Tim Fleming, Deputy Secretary of State, of the issue and called the Director of Elections, Chris Harvey, to determine if the data had been sent from the SDF file.[108]

Mr. Harvey consulted with Kevin Reaves, the Elections System Support Specialist who downloads and burns the SDF, as well as with Mr. Beaver, the CIO.[109] Neither knew how personal identifying information could be included on the SDF.

After speaking with Mr. Harvey, Mr. Beaver consulted with Mr. Cooley who said the inclusion of information on the SDF was impossible. At 4:24 PM on November 13, 2015, Mr. Cooley emailed Mr. Patel stating:

> *Keval, call me right away. Its* [sic] *about the statewide file. Your team did not remove the ssn and dl from the file when it was incorrectly added to the file for the dor interface. Call me. This is an emergency. Brian is being called.*[110]

At 4:41 PM, Mr. Cooley emailed Mr. Beaver the email thread from October 13, 2015 between Mr. Cooley and Mr. Patel, thereby informing Mr. Beaver of the October data transfer.[111]

At 6:56 PM, Mr. Cooley emailed Mr. Beaver and Tim Fleming, Deputy Secretary of State, stating "I have verified that the current statewide file <u>does not</u> have any of the sensitive fields in the file."[112]

---

[107] *Id*.
[108] **Exhibit A**, Statement of Chris Harvey.
[109] *Id*.
[110] *See*, **Exhibits F & J**.
[111] *Id*.
[112] *Id*. (emphasis in original).

November 17, 2015

After an initial investigation, Mr. Fleming reported to Secretary Kemp that Mr. Cooley had been the root cause of the release of data within the Secretary of State's Office. This determination was made based on Mr. Cooley's cover-up of the October incident and failure to follow IT policies and procedures.

In light of these findings, Secretary Kemp terminated Mr. Cooley's employment with his office.

CONCLUSION

With respect to the data release actions, this investigation focuses on the Elections Division and Information Technology (IT) Division. In review of this matter and considering the relevant facts presented through information gathering as listed on page three (3) under Methodology, the investigation yields the following summary and recommendations.

Elections Division

Public voter registration data is distributed by the Elections Division. State law as well as internal processes in the Elections Division guide how this information is distributed. At the time of this incident, requests could be made individually or information could be provided on a recurring basis to a registered entity. Staff process the requests and distribute the information via established protocol. The position that has direct responsibility for this area is the Elections System Support Specialist.

Although one-on-one training had been provided to the Elections Systems Support Specialist, the training process for downloading the SDF was not available in written form. Additionally, the job description for the Elections Systems Support Specialist suggests this position has the responsibility to open files and review the information contained therein before distribution. However, the Elections System Support Specialist is unable to open very large files, over one gigabyte of data. Although, the Elections Systems Manager made a request to Mr. Cooley to provide at least the means of read only access to these large files [the SDF], Mr. Cooley did not provide assistance to comply with this request.

Information Technology Division

The IT Division is responsible for helping to accommodate some requests for voter registration information to state agencies. The guiding policy is the Data Distribution and

Exchange Policy # SOS-ITP-36-3. The IT Governance section processes these requests based on written policy and procedure. *See*, **Exhibit C**. A project manager is assigned to each project created in the IT Division. The Project Manager's job is to apply written practices to guide the project through testing and release management. Stakeholders are generally involved in this process and Senior IT Management receives weekly project updates. Project timelines and progress are tracked electronically through JIRA, and stakeholders have access to this system.

From a process perspective, an anomaly existed with ad-hoc requests. These requests were allowed to be fast-tracked around the normal IT Governance process. Further, the Systems Programmer III position (previously held by Mr. Cooley) was able to push these requests through and provide directives to an approved Secretary of State vendor for file changes. This level of autonomy enabled this position to change the scope request and to request information to be added or deleted from a data file. This activity is outside the IT Governance policies. The guiding policies are clear, well-written, and have the safeguards in place to prevent a data release.

Collectively, after considering all available information, the data release issue internally was due to Mr. Cooley working outside of and circumventing established policies and procedures. Mr. Cooley provided communication to PCC to add three fields to a statewide voter list. Although Mr. Cooley admits that it was not his intention to have this additional information included in the SDF, his written directive to PCC did not clearly convey his intention. Additionally, access to the file folder that housed this information was provided from PCC to Mr. Cooley only. This process was established to limit access to confidential information and to control data release. As a general practice, this working folder allowed PCC to make changes to files, upload the draft and allow Mr. Cooley to review data to ensure the file contained the correct information. Once reviewed, Mr. Cooley could approve the download of information to a SFTP site.

PCC's access authorization practice provides safeguards related to data management. However, to further complicate the data release issue, Mr. Cooley circumvented another policy by sharing his log-on and password information to allow an employee of the Elections Division to have access to this confidential file folder. This Elections Division employee is required to process approved voter list requests. However, no Elections Division employee should have access to this confidential file folder.

Lastly, approximately seven days after the file was loaded on the secure SFTP site, Mr. Cooley found the error that information containing confidential information was added to the SDF and contacted PCC to remove the information from the file. PCC complied and Mr. Cooley states that he checked the system to see if anyone accessed the file. Mr. Cooley did not alert anyone else regarding the issue. However, this file was on the secure SFTP site for approximately seven days before this error was found, and during this time Mr. Cooley's credentials as provided by him to the Elections Division employee were used to access and download the SDF onto a CD to distribute to registered recipients. The Elections Division employee provided this CD of the SDF on a monthly basis, and the information contained within the normal SDF did not contain confidential information such as social security numbers or dates of birth. Neither the Elections Division employee nor the Division's management were aware of the file error and had no reason to believe that the additional data had been added to the SDF.

This investigation concludes that, collectively, there is a need for process improvement through adopting additional policies and procedures relevant to data release.

Further, management should be involved in disseminating policies to employees as well as providing formal training to staff to ensure procedural understanding and compliance. It is imperative that management take a collaborative stakeholder approach with respect to

communication when divisions share or take part in joint functions, to include policy, procedure, or project hand-off.

ACTION ITEMS

Elections Division

- Formal implementation of December 2015 Elections Data Release Policy and Standard Operating Procedures. *See*, **Exhibit K**.
- Management to be involved in formal rollout of data release policy and procedures to employees to ensure procedural understanding.
- Management to be directly involved as a collaborative stakeholder with respect to meetings, information dissemination and communication when divisions share or a take part in a joint function, policy, procedure, project or data release.
- Implement data release cross-check redundancies to include managerial review.

Information Technology Division

- Provide formal training to all Secretary of State staff regarding data management and release.
- Management to be directly involved as a collaborative stakeholder with respect to meetings, information dissemination and communication when divisions share or a take part in a joint function, policy, procedure, project or data release.
- Provide appropriate and timely communication to a Division Director or designee when IT is working on a request or project that has any overlap with another division.
- Implement data release cross-check redundancies to include managerial review.
- Discontinue the work-around practice regarding ad-hoc requests, and follow the established IT Governance policies and processes.

- CIO to disallow lower level positions unilateral approval authority related to providing directives to vendors, approving contracts and/or changes in scope, the approval to alter or deliver critical, sensitive, or confidential information, and ensure approved Secretary of State policies and procedures are not circumvented.
- CIO and appointed Secretary of State senior staff to have joint involvement in the approval of emergency data requests, changes to project scope, or any request to provide, alter or deliver critical, sensitive, or confidential information.
- IT senior management to draft and present to Secretary of State senior staff redundant safeguards on governance to include risk mitigation of intentional or unintentional release of critical information or files.
- All IT staff to follow approved procedures.
- Provide training to all Secretary of State staff regarding the official data release policies and procedures.

INDEX TO EXHIBITS

A. Employee Statements

B. Job Descriptions

C. IT Policies

D. SANS Report

E. PCC Documents

F. Emails Related to the Department of Revenue Request

G. JIRA Tickets

H. Voter List Requests

I. Gary Cooley's Personnel File

J. Gary Cooley's Emails

K. Remedial Documents